Universiti Teknologi MARA

A Signature Based Intrusion Detection System (IDS) : Using Snort

Nik Mariza Nik Abdul Malik

Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science
Faculty of Information Technology & Quantitative Science

February 2004

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH,
(AL MIGHTY) THE GRACIOUS, THE MOST MERCIFUL

Alhamdulillah, with His will has allowed me to complete this research.

First and foremost, I would like to express my special gratitude to my principal supervisor, PM Dr Saadiah Yahya for her guidance, advice, co-operation, useful ideas and encouragement in order to complete this research.

I would like to dedicate deep appreciation to my co-supervisor, Encik Abdul Hamid Othman who had given very good technical guidance, valuable suggestions and moral support throughout the completion of this research.

My appreciation also goes to the Coordinator of Master In Science (Information Technology) (by Research), Dr Arsmah Hj. Ibrahim for her effort to ensure her students are always comfortable with the research environment.

Very special thanks also go to Puan Salmah, Network Administrator in FTMSK and all of her staff for their co-operation in giving information and permission to use the computer laboratory for the research.

Lastly, to my beloved husband and family who always prays for my success in my studies in UiTM. Not to forget, special thanks to lecturers and to all my friends for their support and those who were involved whether directly or indirectly in helping me to finish this research.

Without help and support from all those mentioned above, it would have been impossible to complete this research. Thank you very much.

TABLE OF CONTENTS

	Page
AKNOWLEDGEMENTS	**ii**
LIST OF TABLES	**vi**
LIST OF FIGURES	**vii**
LIST OF ABBREVIATIONS	**x**
ABSTRACT	**xi**
CHAPTER	
1 INTRODUCTION	**1**
1.1 Introduction	1
1.2 Background	2
1.3 Problem Description	6
1.4 Objective of the Research	9
1.5 Research Scope	9
1.6 Research Benefits	10
1.7 Organization of Thesis	10
1.8 Limitation of the Research	11
1.9 Conclusion	11
2 LITERATURE REVIEW	**12**
2.1 Introduction	12
2.2 Prior Art in Intrusion Detection System	12
2.3 Approaches to Intrusion Detection Systems (IDS)	14
2.3.1 Basic Deployment Strategies	14
2.3.2 Methods of Detection	16
2.4 Signature Based IDS	23
2.4.1 Prior Art in Signature Based IDS	24
2.4.2 Signature Based IDS in Relation to TCP/IP	26
2.4.3 Snort as a Signature Based IDS	27
2.5 Conclusion	28

ABSTRACT

Intrusion detection has become the main issue to consider by any organization transporting sensitive and confidential information over the network. This is because those organizations are exposed to intruders. Intrusion Detection Systems (IDS) are software or hardware systems that automate the process of monitoring intrusion events that occur in a computer system or network, and analyze them for signs of intrusions. Today, the number of IDS has increased rapidly. Most IDS are signature based, which means that they make use of a certain pattern of a packet to identify intrusion in the network traffic. This pattern of a packet is also known as 'signature'. This signature needs to be up-to-date to ensure that the IDS is working properly and able to identify the pattern of interest. The task of updating signature can either be done by network administrator or using the default installation installed by the IDS vendor. Therefore, the objective of this research is to simulate the actual process involved in identifying a signature to write a rule. It uses a signature based IDS named Snort that is capable of detecting an intrusion using a signature, which is embedded in its rule sets. This research is done in a controlled laboratory environment, which consists of small Local Area Network (LAN).

As a result of this research, seven steps have been identified in the process of identifying the signature of a packet to write a rule. This rule is used to detect the abnormal packet, which is a possible intrusion packet for the respective implemented network environment.

CHAPTER 1

INTRODUCTION

1.1 Introduction

The Internet supports a vast and growing community of computer users around the world. In this world of global communications, the importance of network security has increased. Network security is an approach to protect the network from unauthorized users or intruders by network administrators, in keeping network resources safe. Today, it has been one of the most important topics in network management. This is because, the explosive use of Internet has lead to the increasing number of intrusion. It is due to the availability of information on how to intrude and intrusion tools, which can be freely downloaded from the Internet. Even there are websites that are dedicated for hackers. To make the situation worse, intruders are getting smarter. These are the reasons why intrusion becomes significant, today.

New system vulnerabilities, configuration problems and different type of intrusions have been discovered daily, and professionals in the computer field continue to seek ways to identify and stop the intruders. According to Northcutt et al. (2003), there are six important aspects or components of network security that can properly defend a network, that are router, firewall, Intrusion Detection System (IDS), Virtual Private Networks (VPN), software architecture and De-Militarized Zones (DMZ). One of the components of network security that capable to respond to or provide real-time detection and alert of an intrusion attempt is called an Intrusion Detection System (IDS).